CRAzoom

"The Buzz on Accreditation and Compliance"

PBSA Accreditation is shifting from a benefit to a necessity for employers when choosing or retaining their employment screening partner. Unaccredited employment screening firms limit their opportunities and increase their liabilities. Compliance in our regulated and litigious industry continues to be critical for CRAs and, their clients. CRA vendors are increasingly implementing "know your client" audits and reviews. CRAzoom helps employment screening CRAs address these challenges quickly and efficiently.

Remote Workforce Policy

The COVID pandemic changed some things temporarily and some things for the immediate future. One of the things that has not gone back to pre-pandemic levels is the increased use of a more remote workforce.

We've discussed in the past few articles how having remote workers does not prohibit PBSA Accreditation, but there does need to be a secure physical office space that is not a private home. There are also proposed changes to the PBSA accreditation standard that address the remote workforce security environment. I anticipate these changes will go through will little change. These changes will require a written remote workforce policy.

Regardless of your PBSA Accreditation status or plans, if you have remote workers, you should have a remote worker policy to ensure that your company's security protocols and expectations are met. In fact, it may be more important as remote workers may work in a less supervised environment. And vendors and clients are increasingly wanting your written affirmation of security measures—including remote workers.

Prior to crafting a policy, you may want to consider classifying your workers by the duties they perform and the access to Personally Identifiable Information to which they have access. A worker who is processing consumer reports within your system is different than a salesperson without access to PII. As a CRA, you have workers that perform sales and administrative duties, but a significant part of your workforce is dealing with processing personal and sensitive information. Different duties require different levels of security.

> ***"if you have remote workers, you should have a remote worker policy to ensure that your company's security protocols and expectations are met."***

For all workers, you should have a policy and procedures that addresses:

- The collection,
- Handling, and
- Disposal of personal information
- Acceptable use of IT systems and devices.
- Duty and responsibility for the confidentiality and safeguarding of sensitive information.
- General practices, rules, and regulations to maintain information security.
- Risk management, records management, and retention.
- Data processing practices and accountability of each employee.
- Initial and periodic training and supervision of staff in handling personal data. This is included in our training as outlined in our Policy and Procedure 6.11 Worker Confidentiality, Legal, and Compliance Training.

For remote workers, you should emphasize that safe information storage and handling policies and practices are still in place and are more important than ever to observe. Of particular importance while working remotely/at home is to be aware and take precautions in the following areas:

- Others present in the home environment: Be aware of other people in the household who are not authorized to see what is on the worker's screen or in an open folder and take precautions
- As such, Close and lock devices. For the reasons stat-

Read more

ed above, devices used at home for company business should be closed and locked when not in use.

• Downloading information to a hard or portable drive. Never download PII. Use the secure interface.

• Antivirus software and wi-fi/router should be password protected and are required.

• Paper: While the printing and receiving of paper documents containing PII or other sensitive information are rare, you should shred or lock them.

• Phishing threats are on the rise and you should not open any link or attachment which you did not request.

ABOUT THE AUTHOR

Derek Hinton is President of CRAzoom, a company used by the majority of CRAs to achieve and maintain PBSA Accreditation. In addition, Derek consults as a fractional Compliance Officer for CRAs, has created “plug and play” packages for CRAs being audited by their vendors, and is the owner and creator of CrimApollo, a criminal record assessment tool for employers and CRAs. Derek is also the managing partner of NameGrades, a program that assesses the commonality of names in the United States.